

PATENT APPLICATION

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re the Application of

Ryu INADA et al.

Application No.: 09/987,411

Filed: November 14, 2001

Group Art Unit: 2152

Docket No.: 111121

For: METHOD AND APPARATUS FOR PROCESSING SUBJECT NAME INCLUDED IN
PERSONAL CERTIFICATE

CLAIM FOR PRIORITY

Director of the U.S. Patent and Trademark Office
Washington, D.C. 20231

Sir:

The benefit of the filing dates of the following prior foreign applications filed in the following foreign country is hereby requested for the above-identified patent application and the priority provided in 35 U.S.C. §119 is hereby claimed:

Japanese Patent Application No. 2001-315276 filed October 12, 2001

Japanese Patent Application No. 2000-350185 filed November 16, 2000

In support of this claim, certified copies of said original foreign applications:

 X are filed herewith.

 were filed on in Parent Application No. filed .

 will be filed at a later date.

It is requested that the file of this application be marked to indicate that the requirements of 35 U.S.C. §119 have been fulfilled and that the Patent and Trademark Office kindly acknowledge receipt of these documents.

Respectfully submitted,

James A. Oliff
Registration No. 27,075

Joel S. Armstrong
Registration No. 36,430

JAO:JSA/mlb

Date: December 26, 2001

OLIFF & BERRIDGE, PLC
P.O. Box 19928
Alexandria, Virginia 22320
Telephone: (703) 836-6400

**DEPOSIT ACCOUNT USE
AUTHORIZATION**

Please grant any extension
necessary for entry;

Charge any fee due to our
Deposit Account No. 15-0461

RECEIVED
DEC 28 2001
Technology Center 2100

RECEIVED
SEP 10 2002
Technology Center 2100

RECEIVED
JAN 03 2002
TC 1700



#4



日 本 国 特 許 庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office

出 願 年 月 日

Date of Application:

2001年10月12日

出 願 番 号

Application Number:

特願2001-315276

出 願 人

Applicant(s):

富士ゼロックス株式会社

RECEIVED
DEC 28 2001
Technology Center 2100

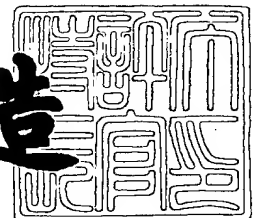
RECEIVED
JAN 03 2002
TC 1700

RECEIVED
SEP 10 2002
Technology Center 2100

2001年12月 7日

特許庁長官
Commissioner,
Japan Patent Office

及川耕造



出証番号 出証特2001-3106900

【書類名】 特許願

【整理番号】 FE01-01395

【提出日】 平成13年10月12日

【あて先】 特許庁長官殿

【国際特許分類】 G06F 17/60

【発明の名称】 個人証明書サブジェクト名処理装置および方法

【請求項の数】 19

【発明者】

 【住所又は居所】 神奈川県川崎市高津区坂戸3丁目2番1号 K S P R
 & D ビジネスパークビル 富士ゼロックス株式会社内

 【氏名】 稲田 龍

【発明者】

 【住所又は居所】 神奈川県川崎市高津区坂戸3丁目2番1号 K S P R
 & D ビジネスパークビル 富士ゼロックス株式会社内

 【氏名】 黒崎 雅人

【特許出願人】

 【識別番号】 000005496

 【氏名又は名称】 富士ゼロックス株式会社

 【電話番号】 0462-38-8516

【代理人】

 【識別番号】 100086531

 【弁理士】

 【氏名又は名称】 澤田 俊夫

 【電話番号】 03-5541-7577

【選任した代理人】

 【識別番号】 100093241

 【弁理士】

 【氏名又は名称】 宮田 正昭

【選任した代理人】

【識別番号】 100101801

【弁理士】

【氏名又は名称】 山田 英治

【先の出願に基づく優先権主張】

【出願番号】 特願2000-350185

【出願日】 平成12年11月16日

【手数料の表示】

【予納台帳番号】 038818

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【包括委任状番号】 9605865

【包括委任状番号】 0006675

【包括委任状番号】 0006676

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 個人証明書サブジェクト名処理装置および方法

【特許請求の範囲】

【請求項 1】 個人証明書に含まれるサブジェクト名を処理する個人証明書サブジェクト名処理装置において、

個人証明書を受信する手段と、

受信した個人証明書を電子署名技術に基づいて検証する手段と、

受信した個人証明書に含まれるサブジェクト名の階層中の少なくとも 1 つの所定のエレメントを抽出する手段と、

上記検証が成功したときに、上記所定のエレメントの値に基づいて、上記個人証明書の保持者のアクセス権限を決定する手段とを有することを特徴とする個人証明書サブジェクト名処理装置。

【請求項 2】 上記所定のエレメントのうちの 1 つは、上記サブジェクト名の所定階層のオーガニゼーショナル・ユニット・ネームである請求項 1 記載の個人証明書サブジェクト名処理装置。

【請求項 3】 上記所定のエレメントは、業務のプロジェクト名を表すために割り当てられた 1 の階層のオーガニゼーショナル・ユニット・ネームと、目的を表すために割り当てられた、コモンネームの一部とする請求項 1 記載の個人証明書サブジェクト名処理装置。

【請求項 4】 個人証明書を受信する手段と、

受信した個人証明書を電子署名技術に基づいて検証する手段と、

受信した個人証明書に含まれるサブジェクト名の階層中の少なくとも 1 つの所定のエレメントを抽出する手段と、

受信した個人証明書の検証が成功したときに、上記所定のエレメントの値に基づいて、上記個人証明書の保持者のアクセス権限を決定する手段とを有することを特徴とするウェブ・サーバ・コンピュータ・システム。

【請求項 5】 個人証明書を受信する手段と、

受信した個人証明書を電子署名技術に基づいて検証する手段と、

受信した個人証明書の検証が成功したときに、セッション識別子を割り当てる

手段と、

受信した個人証明書に含まれるサブジェクト名の階層中の少なくとも1つの所定のエレメントを抽出する手段と、

受信した個人証明書の検証が成功したときに、上記所定のエレメントの値に基づいて、上記個人証明書の保持者のアクセス権限を決定する手段と、

決定したアクセス権限を上記セッション識別子に関連づけて保持する手段とを有することを特徴とするウェブ・サーバ・コンピュータ・システム。

【請求項6】 上記所定のエレメントのうちの1つは、上記サブジェクト名の所定階層のオーガニゼーショナル・ユニット・ネームである請求項5記載のウェブ・サーバ・コンピュータ・システム。

【請求項7】 上記所定のエレメントは、業務のプロジェクト名を表すために割り当てられた1の階層のオーガニゼーショナル・ユニット・ネームと、目的を表すために割り当てられた、コモンネームの一部とする請求項5記載のウェブ・サーバ・コンピュータ・システム。

【請求項8】 サブジェクト名の所定のエレメントが保持者の所属組織および個人ID以外の属性を表す個人証明書を受信して当該サブジェクト名を処理する個人証明書サブジェクト名処理装置において、

上記個人証明書を受信する手段と、

受信した個人証明書に含まれるサブジェクト名の階層中の所定のエレメントを抽出する手段と、

少なくとも、上記所定のエレメントの値が表す、保持者の所属組織および個人ID以外の属性に基づいて、アクセス権限を決定する手段とを有することを特徴とする個人証明書サブジェクト名処理装置。

【請求項9】 上記サブジェクト名の所定階層のオーガニゼーショナル・ユニット・ネームが、保持者がオーガニゼーション・ネームが表す組織の構成員ではなく、かつ当該組織に対して協力していることを示す請求項8記載の個人証明書サブジェクト名処理装置。

【請求項10】 上記サブジェクト名の所定階層のオーガニゼーショナル・ユニット・ネームが、保持者が参加するプロジェクト名を表す請求項8記載の個

人証明書サブジェクト名処理装置。

【請求項 1 1】 上記サブジェクト名の所定階層のオーガニゼーショナル・ユニット・ネームが、オーガニゼーション・ネームが表す組織に対して協力し、かつ保持者が属する、協力組織名を表す請求項 8 記載の個人証明書サブジェクト名処理装置。

【請求項 1 2】 上記サブジェクト名の所定階層のオーガニゼーショナル・ユニット・ネームが、保持者が参加する業務の種類を表す請求項 8 記載の個人証明書サブジェクト名処理装置。

【請求項 1 3】 上記サブジェクト名のコモンネームが、保持者が参加する業務の種類を表す請求項 8 記載の個人証明書サブジェクト名処理装置。

【請求項 1 4】 個人証明書を受信する手段と、
受信した個人証明書に含まれるサブジェクト名の階層中の所定のエレメントを抽出する手段と、

上記所定のエレメントの値に基づいてアクセス権限を決定する手段とを有することを特徴とする個人証明書サブジェクト名処理装置。

【請求項 1 5】 個人証明書に含まれるサブジェクト名を処理する個人証明書サブジェクト名処理方法において、

個人証明書を受信するステップと、

受信した個人証明書を電子署名技術に基づいて検証するステップと、

受信した個人証明書に含まれるサブジェクト名の階層中の少なくとも 1 つの所定のエレメントを抽出するステップと、

上記検証が成功したときに、上記所定のエレメントの値に基づいて、上記個人証明書の保持者のアクセス権限を決定するステップとを有することを特徴とする個人証明書サブジェクト名処理方法。

【請求項 1 6】 サブジェクト名の所定のエレメントが保持者の所属組織および個人 ID 以外の属性を表す個人証明書を受信して当該サブジェクト名を処理する個人証明書サブジェクト名処理方法において、

上記個人証明書を受信するステップと、

受信した個人証明書に含まれるサブジェクト名の階層中の所定のエレメントを

抽出するステップと、

少なくとも、上記所定のエレメントの値が表す、保持者の所属組織および個人 I D 以外の属性に基づいて、アクセス権限を決定するステップとを有することを特徴とする個人証明書サブジェクト名処理方法。

【請求項 1 7】 個人証明書に含まれるサブジェクト名を処理するためにコンピュータに用いられる個人証明書サブジェクト名処理用コンピュータ・プログラムにいて、

個人証明書を受信するステップと、

受信した個人証明書を電子署名技術に基づいて検証するステップと、

受信した個人証明書に含まれるサブジェクト名の階層中の少なくとも 1 つの所定のエレメントを抽出するステップと、

上記検証が成功したときに、上記所定のエレメントの値に基づいて、上記個人証明書の保持者のアクセス権限を決定するステップとをコンピュータに実行させるために用いられることを特徴とする個人証明書サブジェクト名処理用コンピュータ・プログラム。

【請求項 1 8】 サブジェクト名の所定のエレメントが保持者の所属組織および個人 I D 以外の属性を表す個人証明書を受信して当該サブジェクト名を処理するためにコンピュータに用いられる個人証明書サブジェクト名処理用コンピュータ・プログラムにおいて、

上記個人証明書を受信するステップと、

受信した個人証明書に含まれるサブジェクト名の階層中の所定のエレメントを抽出するステップと、

少なくとも、上記所定のエレメントの値が表す、保持者の所属組織および個人 I D 以外の属性に基づいて、アクセス権限を決定するステップとをコンピュータに実行させるために用いられることを特徴とする個人証明書サブジェクト名処理用コンピュータ・プログラム。

【請求項 1 9】 サブジェクト名のオーガニゼーショナル・ユニット・ネームおよびコモン・ネームの少なくとも 1 つが保持者の所属組織および個人 I D 以外の属性を表す個人証明書を記録したコンピュータ読取り可能な記録媒体。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

この発明は、個人証明書（以下では単に証明書と呼ぶこともある）のサブジェクト名を利用してアクセスを制御する技術に関する。

【0002】

【従来の技術】

ITU-T勧告X.509はディレクトリモデル認証を規定しており、このディレクトリモデル認証に準拠して個人証明書を発行局（認証局）から発行してもらう。発行局は申請人から証明書の発行に必要な情報（名前、所属、公開鍵等）を受け取り所定のポリシーに従い証明書を発行し、証明書を所定の証明書格納部に保存する。申請人は証明書格納部から証明書を取り出すことができる。

【0003】

ところで、個人証明書のサブジェクト名をただだけでは、その証明書の保持者がどういう権限を有しており、どういう性質をもっているか不明である。保持者が有している権限や性質を知るために種々のアプローチが採用されている。例えば、証明書のサブジェクト名と権限とをデータベースに登録し、証明書を用いたアクセスがあるたびにデータベースに問合せる。しかしこの方法は効率の面で問題があった。

【0004】

図10は、上述の従来のアプローチを実現するシステム例を示している。この図において、ユーザはクライアント端末500を用いてネットワーク（例えばインターネット）501を介してウェブ・サーバ502にアクセスする。このアクセスはSSL手法を用いて行われ、クライアント端末500およびウェブ・サーバ502の間で証明書を交換し、認証を行い、この後、ネゴシエーションにより決定された慣用暗号によりデータを暗号化して送受信する。ウェブ・サーバ502は、クライアント端末500から送られた証明書のサブジェクト名（証明書に記載されている被認証者の識別子）を用いてデータベースサーバ（ディレクトリサービス）503に問い合わせクライアント端末500のユーザがアクセス権限

を有するかどうかを知る。例えば、アクセス対象の権限レベル（例えば0、1、2等）とサブジェクト名を引数としてデータベースサーバ503に問い合わせ、当該サブジェクト名のユーザが当該権限レベルにアクセスできるかどうかを応答として受け取る。データベースサーバ503は、ユーザ（サブジェクト名）と許容されている権限レベルとの関係を記憶保持している。もちろん、サブジェクト名を引数として許容権限レベルを受け取ってウェブ・サーバ502側においてアクセス対象ファイルがその許容権限レベル以内かを判別するようにすることもあるし、サブジェクト名とアクセス対象ファイル名（ディレクトリ名）をデータベースサーバ503に引き渡して照会を行ってもよい。

【0005】

以上のような従来のアプローチでは、アクセスのたびにネットワーク501を介してデータベースサーバ503に権限の照会を行うので、計算機コストを消費することになる。また、ネットワーク501に照会データがそのまま送信されるのでセキュリティ上問題がないわけではなかった。

【0006】

また、上述の問題を回避するためにデータベースサーバ503の権限情報のセットまたはサブセットのコピー（データベースサーバ）をウェブ・サーバ500のサイトにローカルに配置することも考えられる。しかし、このようにすると、データベースサーバ503およびそのコピーとの間で一貫性を維持しなければならず、保守管理等が煩雑となる。また、各サイトにデータベースサーバを配置するとコストアップになる。

【0007】

【発明が解決する課題】

この発明は、以上の事情を考慮してなされたものであり、証明書のサブジェクト名から直ちにその権限や性質を知ることができ、これを用いて簡易にアクセス制御等を行える技術を提供することを目的としている。

【0008】

【課題を解決するための手段】

この発明によれば、上述の目的を達成するために、特許請求の範囲に記載のと

おりの構成を採用している。ここでは、発明を詳細に説明するのに先だって特許請求の範囲の記載について補充的に説明を行っておく。

【 0 0 0 9 】

この発明の一側面によれば、上述の目的を達成するために、個人証明書に含まれるサブジェクト名を処理する個人証明書サブジェクト名処理装置に：個人証明書を受信する手段と；受信した個人証明書を電子署名技術に基づいて検証する手段と；受信した個人証明書に含まれるサブジェクト名の階層中の少なくとも1つの所定のエレメントを抽出する手段と；上記検証が成功したときに、上記所定のエレメントの値に基づいて、上記個人証明書の保持者のアクセス権限を決定する手段とを設けるようにしている。

【 0 0 1 0 】

この構成においては、個人証明書を認証してそのサブジェクト名のエレメントの真正を確認し、この真正なエレメントの値に基づいてアクセス権限を判別することができ、ディレクトリサービス等のデータベースにアクセスする必要がなくなる。

【 0 0 1 1 】

この発明の他の側面によれば、上述の目的を達成するために、ウェブ・サーバ・コンピュータ・システムに：個人証明書を受信する手段と；受信した個人証明書を電子署名技術に基づいて検証する手段と；受信した個人証明書に含まれるサブジェクト名の階層中の少なくとも1つの所定のエレメントを抽出する手段と；受信した個人証明書の検証が成功したときに、上記所定のエレメントの値に基づいて、上記個人証明書の保持者のアクセス権限を決定する手段とを設けるようにしている。

【 0 0 1 2 】

この構成においても、ディレクトリサービス等のデータベースを利用することなく簡易にアクセス権限を判別することができる。

【 0 0 1 3 】

ウェブ・サーバ・コンピュータ・システムはウェブ・サーバ単体で構成されてもよく、ウェブ・サーバとアプリケーション・サーバとで構成されてもよい。ア

クセス権限の判別を行うために各種の機能はウェブサーバの認証機能やCGI（コモンゲートインタフェース）プログラムや、アプリケーション・サーバにより実現される。

【0014】

この発明のさらに他の側面によれば、上述の目的を達成するために、サブジェクト名の所定のエレメントが保持者の所属組織および個人ID以外の属性を表す個人証明書を受信して当該サブジェクト名を処理する個人証明書サブジェクト名処理装置に：上記個人証明書を受信する手段と；受信した個人証明書に含まれるサブジェクト名の階層中の所定のエレメントを抽出する手段と；上記所定のエレメントの値が表す、保持者の所属組織および個人ID以外の属性に基づいて、アクセス権限を決定する手段とを設けるようにしている。

【0015】

この構成においては、ディレクトリサービス等のデータベースを利用することなく簡易にアクセス権限を判別することができる。とくにサブジェクト名のオーガニゼーショナル・ユニット・ネームを利用することにより柔軟にアクセス権限情報を規定できる。

【0016】

なお、この発明は装置やシステムとして実現できるのみでなく、方法としても実現できる。またこのような方法の一部をコンピュータプログラムとして実現してもよい。

【0017】

この発明の上述の各側面およびこの発明の他の側面は特許請求の範囲に記載され、以下、実施例を用いて詳細に説明される。

【0018】

【発明の実施の形態】

以下、この発明を情報アクセスシステムに適用した実施例について説明する。この実施例は、幹事会社と協力会社とが所定のプロジェクト名の下で協力して事業を行うことを前提とし、幹事会社および協力会社の従業者等が幹事会社の情報にアクセスできるようにするものである。情報のアクセスには個人証明書を利用

する。幹事会社は、個人証明書の発行にイニシャティブを持つ会社（事業体）である。もちろん、この発明は、このような環境下のみでなく、情報をアクセスする際に権限を判別する種々の環境下で適用可能である。上述の幹事会社ではなく、証明書の発行を業とする認証局が、証明書を発行するような環境下でも適用可能である。

【0019】

図1は、この実施例の情報アクセスシステムを示しており、この図において、証明書発行センタ（幹事会社サイト）10、協力会社サイト20等がインターネット30に接続されている。ここでは、便宜上、証明書発行センタ10は、幹事会社の社内に設けられているものとする。協力会社サイト20は、構内ネットワーク網（LAN）等によりイントラネットを構築しており、各イントラネットにクライアント端末201が接続されている。

【0020】

この例において、証明書発行センタ10は、協力会社サイト20のクライアント端末201等からの個人証明書発行申請を受け取って個人証明書の発行処理を行うものである。個人証明書はITU-T勧告X.509に準拠するものであり、図2に示すようなものである。

【0021】

証明書発行センタ10は、ウェブ・サーバ101、アプリケーション・サーバ102、データベース管理システム103、メールサーバ104、クライアント端末105、ルータ106等を有している。これらコンピュータリソースはLAN107に接続されている。

【0022】

ウェブ・サーバ101は、HTTP（ハイパーテキストトランスファプロトコル）プロトコルに従ってクライアント（クライアント端末201、105）から要求を受け取り、要求に応じたHTML文書（XML文書）をクライアントに転送する。アプリケーション・サーバ102は、ウェブ・サーバ101を介してクライアントから送られたプログラム名および引数に基づいて種々の処理を実行するものである。アプリケーション・サーバ102にかえてウェブ・サーバ101

のCGI（コモンゲートインタフェース）のプログラム等を用いてもよい。データベース管理システム103は、証明書発行に関連する種々のデータベースを管理するものである。データベースは、例えば、証明書データベース103a等である。

【0023】

データベース管理システム103が管理する証明書データベース103aに保持される証明書情報の簡略化した例を図3に示す。ここでは、証明書情報について説明する前に、この例で用いるDN（ディステイングイシュトネーム、以下サブジェクト名とも呼ぶ。X.501）について説明しておく。この例では、サブジェクト名は、カントリネーム（C）、オーガニゼーションネーム（O）、第1オーガニゼーションナルユニットネーム（OU1）、第2オーガニゼーションナルユニットネーム（OU2）、第3オーガニゼーションナルユニットネーム（OU3）、コモンネーム（CN）により規定される。幹事会社以外の申請者に対してはOU1として例えば「Partner」等が記述される。幹事会社の社員については、OU1を省略したり、OU1として所定の部門名が記述される。OU2は、プロジェクト名が記述される。ただしプロジェクトと関係がない場合にはOU2は省略される。OU3は、協力会社の会社名が記述される。もちろん、幹事会社の内部の者（社員等）に関してはOU3は省略される。このようにして、サブジェクト名を用いてプロジェクトおよび協力会社を記述することができる。なお、OUのサフィックスは、OUの属性に対応して用いており、例えば部門（社外の組織）をあらわすOU1は、部門の階層に応じてさらに階層的な構成を採用してもよい。例えば、「jinji」（人事部）、「jinji1」（第1人事課）等、OU1を複数規定できる。

【0024】

なお、プロジェクトとは一括りに管理される業務や活動であり、ここでは便宜上、幹事会社と他の協力会社との間で行われる業務を指す。プロジェクトとの関連で協力会社が登録される。もちろん、幹事会社内のプロジェクトや非業務的な活動等を「プロジェクト」として扱ってもよい。このようにすることにより組織構成から離れて証明書を発行することが可能となる。

【0025】

サブジェクト名の具体例を説明する。

【0026】

(1) 具体例1

[C=JP, O=XYZ Co., CN=1234 Ryu Inada]

この例では、保持者がXYZ株式会社の社員であり、社員番号が1234で、指名が「Ryu Inada」であることがわかる。

【0027】

(2) 具体例2

[C=JP, O=XYZ Co., OU=Partner, OU=Xnet, OU=ABC Co., CN=1234 001 Taro Fuji]

この例では、保持者は協力会社のABC株式会社の社員であり、プロジェクトXnetに参画し、その業務目的が調達（コモンネームの001が調達を意味する）であり、所属会社の社員番号が1234で、氏名が「Taro Fuji」であることがわかる。

【0028】

(3) 具体例3

[C=JP, O=XYZ Co., OU=Partner, OU=Xnet, CN=1234 Hanako Fuji]

この例では、保持者が派遣社員であり、その派遣社員番号が1234であり、氏名が「Hanako Fuji」であることを示す。協力会社名あるいはプロジェクト名がないことから派遣社員と判断することができる。

【0029】

図1の説明に戻る。データベース管理システム103が管理する証明書データベース103aは、図3に示すように、証明書情報を保持している。図3に示すように、サブジェクト名は(C, O, OU1, OU2, OU3, CN)であり、コモンネームCNは、例えばCN=12345 001 Taro Yamadaである。「12345」は協力会社ABC内の一意の識別子例えば社員番号である。「001」は幹事会社での業務の種別を示すIDである（例えば、調達業

務、試作業務)。「T a r o Y a m a d a」は申請者の氏名である。証明書データベース103aは証明書ID、サブジェクト名(C, O, O U 1, O U 2, O U 3, C N)、有効期限等を保持している。なお、証明書は、サブジェクト名、発行者名、公開鍵、発行者署名等を含むものである。

【0030】

ウェブ・サーバ101、アプリケーション・サーバ102、データベース管理システム103を用いて具体的な証明書発行処理の機能が実現される。クライアントはウェブ・ベースで証明書発行システムの各種の機能を利用できる。

【0031】

メールサーバ104はSMTP (シンプルメールトランスファプロトコル) デーモン等を実行するものであり、メールの配送を行なう。

【0032】

クライアント端末105は、ウェブ・ブラウザを具備し、証明書発行センタ (幹事会社) 10内で証明書発行センタ10のサービスの提供を受ける。

【0033】

クライアント端末201は、協力会社サイト20に配置されたパーソナルコンピュータ、ワークステーション等であり、ウェブ・ブラウザを実装している。クライアント端末201は、証明書発行センタ10が提供する証明書発行システムにアクセスし、雛型登録 (会社登録)、個人証明書発行申請等を行なうことができる。証明書発行センタ10はインターネット30上に公開されているため、適宜ファイヤーウォール等のセキュリティ機構が設けられることが望ましい。証明書の発行自体はこの発明と直接には関係がないので、詳細な説明は省略する。通常の証明書発行所理を採用できることはもちろんである。

【0034】

このような証明書発行センタ10を用いて証明書の発行を申請し、申請が承認され、証明書が発行される。申請者は、証明書IDを通知され、ウェブ・ベースでこれを入力して証明書を取得する。

【0035】

つぎに証明書を利用したアクセス制御について説明する。

【0036】

図4はアクセス制御を行う機構を模式的に示すものである。この機構はウェブ・サーバ101、アプリケーション・サーバ102により実現される。もちろん、ウェブ・サーバ101のCGIプログラムや、J A V Aサーブレット（商標）等を用いてアプリケーション・サーバ102に代替させることができる。

【0037】

図4において、アクセス制御機構は、ルート証明書保持部150、認証部151、エレメント抽出部152、権限判別部153、権限登録部154、セッション管理部155等を含んで構成される。この例では、ウェブ・サーバ101が、ルート証明書保持部150および認証部151を構成する。そして、アプリケーション・サーバ102がエレメント抽出部152、権限判別部153、権限登録部154、セッション管理部155を構成する。

【0038】

認証部151は図5に示すような認証手続をクライアント端末およびウェブ・サーバ101間で実現する。図5の認証手続は通常のSSL/TLSコネクション要求時にウェブ・サーバ101で実行される認証手続であり、図から明らかであるのでとくに説明は行わない。認証部151は、この認証手続の際に、クライアント端末から証明書を受け取る。この証明書は図5に示す認証手続に利用されるとともに、そのサブジェクト名がエレメント抽出部152に供給される。認証部151は、ルート証明書保持部150に保持されているルート証明書の公開鍵を用いて、クライアント端末から受け取った証明書の署名（図2参照）を検証する。検証が失敗したときにはコネクションは拒否される。検証が成功すると、セッション番号（セッションIDともいう）が割り当てられ、アプリケーション・サーバ105のセッション管理部155によりセッション変数が記憶管理される管理される。

【0039】

エレメント抽出部152はサブジェクト名の階層構造を辿って所定のエレメントを抽出する。この例では、OU1が「Partner」であり、OU3に会社名がある場合に、OU2のプロジェクト名、OU3の会社名、CNの業務種別コ

ード（例えば「001」）を抽出する。

【0040】

権限判別部153は図6に示すような区別に従って文書のアクセス権限を決定し、これをセッション番号に割り当てる。図6に示す区別は例えば図7に示すようなテーブルで実装可能であり、権限判別部153がこのようなテーブルを参照して、アクセス可能なファイルやディレクトリを判別する。権限登録部154はセッション番号と権限（権限レベルやアクセス可能なファイル名／ディレクトリ名）との関係をセッション管理部155に登録する。例えば、セッション管理部155のデータベース（図示しない）に図8に示すように登録する。以降、セッションが継続する間、このセッション番号に基づいてアクセス権限が許容される。

【0041】

なお、以上の認証手続や権限制御は、証明書発行センタ（幹事会社サイト）10のウェブ・サーバ101との間でのみ可能なわけではなく、他のウェブ・サーバとの間でも可能であり、また、同様の認証手続や権限制御をその他種々のサーバとの間で実行できることはもちろんである。

【0042】

上述の実施例では、証明書発行センタ10が幹事会社サイトに設けられるようにしたが、図9に示すように、証明書発行センタ10と幹事会社サイト40とを個別に設けてもよいことはもちろんである。図9に示す例では、証明書発行の機能を証明書発行センタ10に割り当て、ウェブベースでサービスを行う機能を幹事会社サイト40に設けている。幹事会社サイト40には上述実施例と同様な権限制御をウェブ・サーバ101で実行する。図9の例ではウェブ・サーバ101自体が認証部151およびルート証明書保持部150を構成し、ウェブ・サーバ101のCGIプログラムがエレメント抽出部152、権限判別部153、権限登録部154、セッション管理部155を構成している。CGIプログラムでなくJAVAサーブレット等を用いてもよい。もちろん、図1に示すようなアプリケーション・サーバを用いてもよい。

【0043】

図 9 においては図 1 と対応する箇所に対応する符号を付し、説明を繰り返さない。

【 0 0 4 4 】

また、上述では、幹事会社と協力会社とが協力してプロジェクトを行う環境を例に挙げて説明を行ったが、任意の形態のサーバとクライアントとの間の権限制御を同様に行えることはもちろんである。

【 0 0 4 5 】

以上説明したようにこの発明によれば個人証明書のサブジェクト名を利用して簡易に保持者の権限や性質を判別でき、簡易にアクセス制御を行うことができる。

【 0 0 4 6 】

すなわち、従来ディレクトリサービスサーバ（データベースサーバ）で管理していたアクセス制限に関する情報を、サブジェクト名の中に、そのオーガニゼーション・ユニット・ネームやコモンネームの一部として埋め込み、その内容の真正を証明書の署名により確認した上で利用させることができ、ディレクトリサーバ等を用いることなくアクセス制限の情報をサーバに供給することが可能になる。サーバ側では、サブジェクト名に埋め込まれた情報と権限との関係を記述したテーブル等を保持するだけで簡易にアクセス権限を知ることができる。

【 0 0 4 7 】

この結果、ディレクトリサーバを用いてアクセス制限を行っていた従来システムの欠点を解消することができる。すなわち、サブジェクト名や権限レベルがネットワーク（例えばインターネット）上を行き交うことがなくなり、また、ディレクトリサーバ等のコピーを各サーバのサイトに配置する必要もなくなる。

【 0 0 4 8 】

なお、この発明は上述の実施例に限定されるものではなくその趣旨を逸脱しない範囲で種々変更が可能である。例えば、上述例では、コモンネームに業務種別のコードを含ませたが、所定階層のオーガニゼーション・ユニット・ネームに含ませても良い。また、この発明のサブジェクト名の構成をアクセス制御以外の用途に用いることもできることは明らかである。

【 0 0 4 9 】

【 発 明 の 効 果 】

以上説明したように、この発明によれば、個人証明書を用いて簡易にアクセス制御等を行うことができる。

【 図 面 の 簡 単 な 説 明 】

【 図 1 】 この発明の実施例を全体として示すシステム図である。

【 図 2 】 上述の実施例で用いる個人証明書を説明する図である。

【 図 3 】 上述実施例の証明書データベースを説明する図である。

【 図 4 】 上述実施例の申請者権限の制御を模式的に説明するブロック図である。

【 図 5 】 上述実施例の認証手続を説明する図である。

【 図 6 】 上述実施例の権限の区別を説明する図である。

【 図 7 】 上述実施例の権限の区別を規定するテーブルの例を説明する図である。

【 図 8 】 上述実施例のセッション管理を説明する図である。

【 図 9 】 上述実施例の変形例を説明する図である。

【 図 1 0 】 従来例を説明する図である。

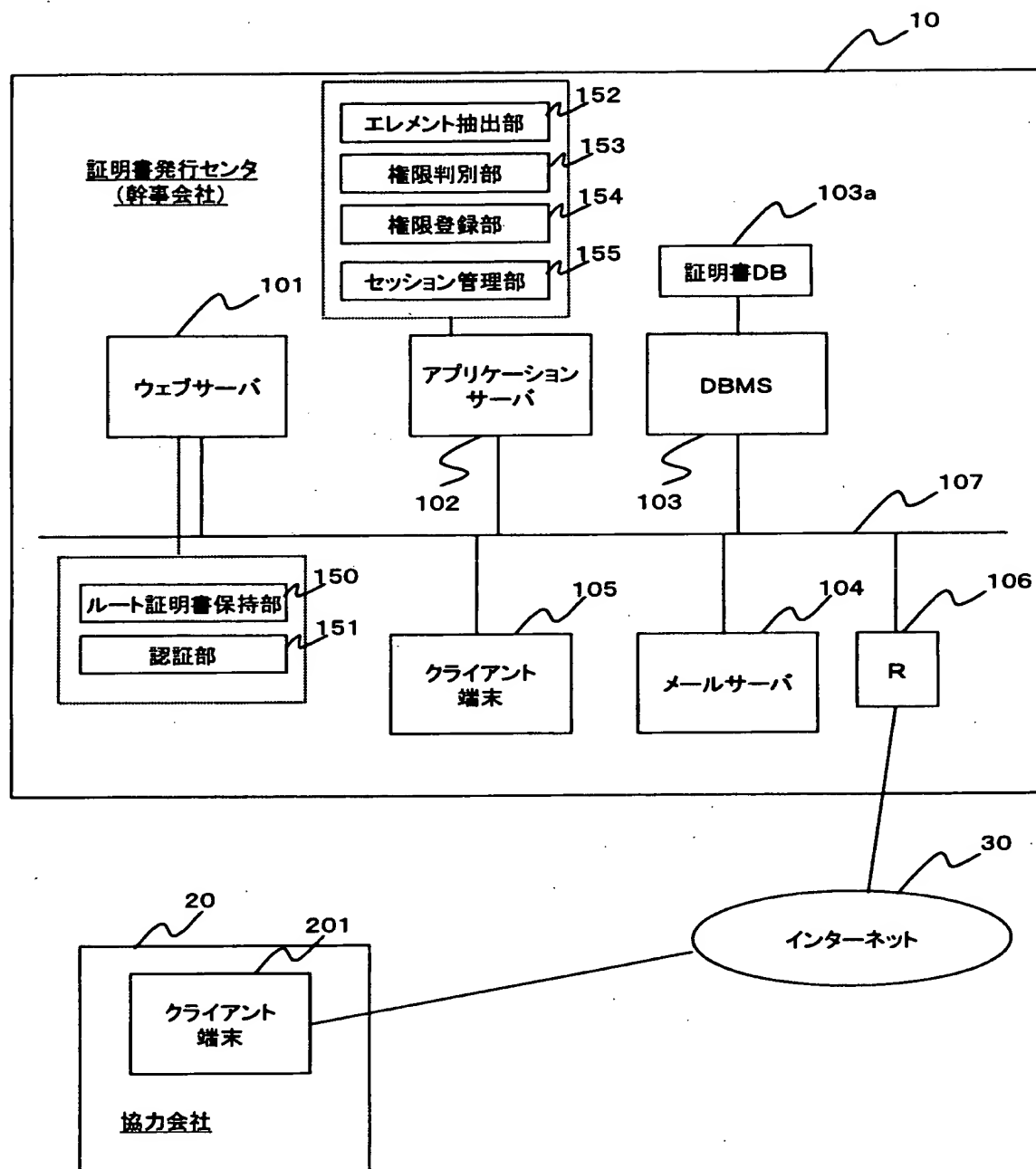
【 符 号 の 説 明 】

- 1 0 証明書発行センタ
- 2 0 協力会社サイト
- 3 0 インターネット
- 4 0 幹事会社サイト
- 1 0 1 ウェブ・サーバ
- 1 0 2 アプリケーション・サーバ
- 1 0 3 データベース管理システム
- 1 0 3 a 証明書データベース
- 1 0 4 メールサーバ
- 1 0 5 アプリケーション・サーバ
- 1 0 5 クライアント端末

1 0 6	ルータ
1 5 0	ルート証明書保持部
1 5 1	認証部
1 5 2	エレメント抽出部
1 5 3	権限判別部
1 5 4	権限登録部
1 5 5	セッション管理部
2 0 1	クライアント端末
5 0 0	クライアント端末
5 0 1	ネットワーク
5 0 2	ウェブ・サーバ
5 0 3	データベースサーバ

【書類名】 図面

【図 1】



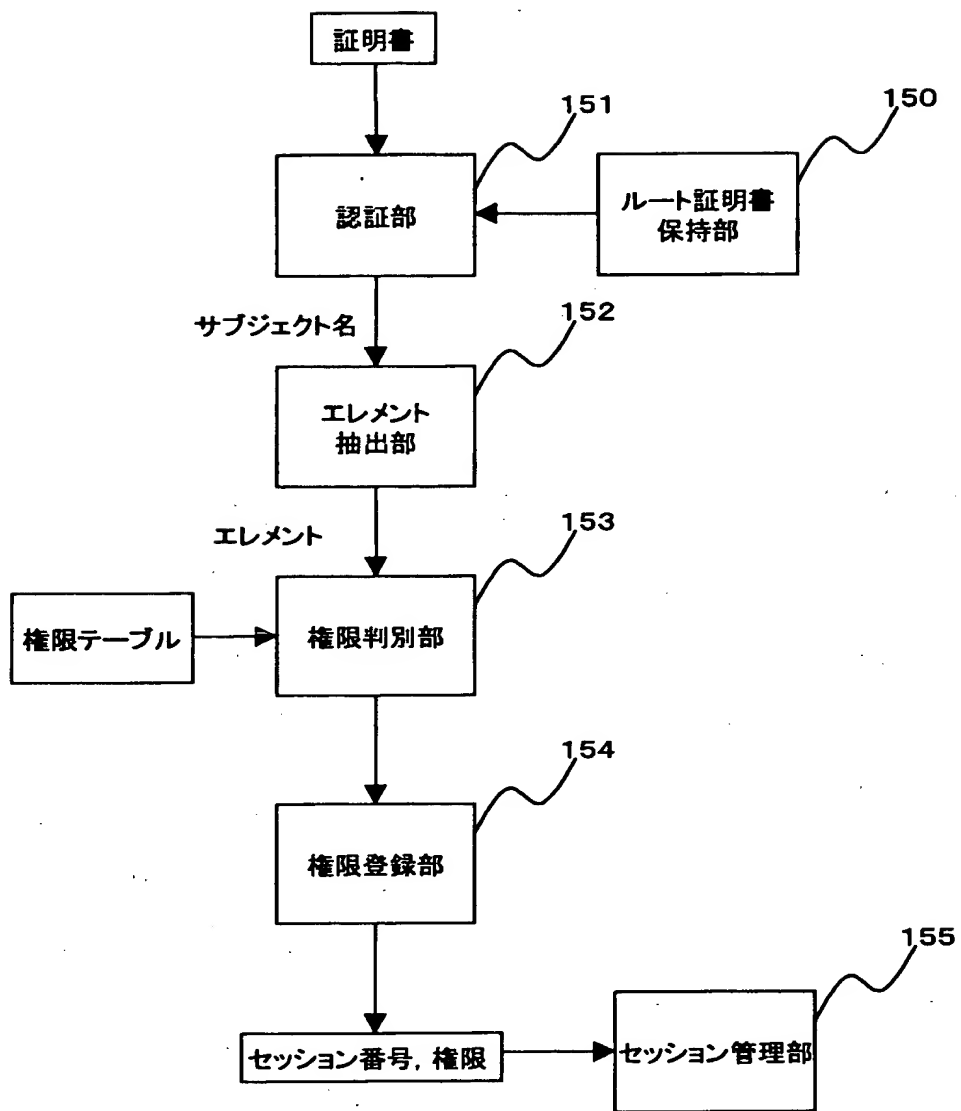
【図 2】

証明書のバージョン
シリアル番号
認証局の識別子
有効期間
サブジェクト名 (被認証者の識別子)
被認証者の公開鍵情報
失効証明書リストの取得情報
認証ポリシーの情報
被認証者が認証局か否か
認証局の署名

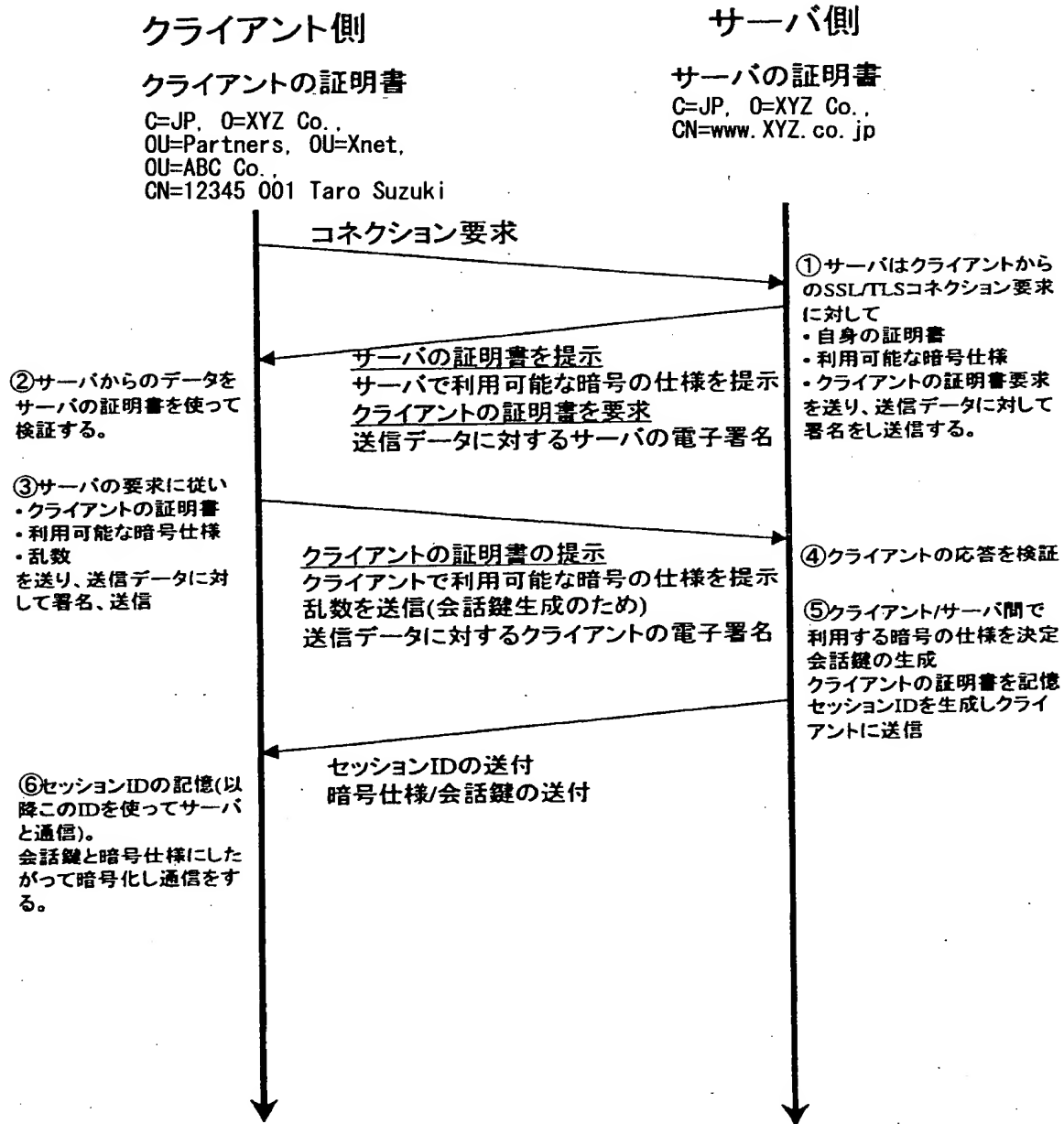
【図 3】

証明書情報			
証明書ID	サブジェクト名	証明書の有効期限	公開鍵
00002	JP, XYZ, Partner, Xnetproject, ABC, 12345 001 Taro Yamada	2000/12/31	

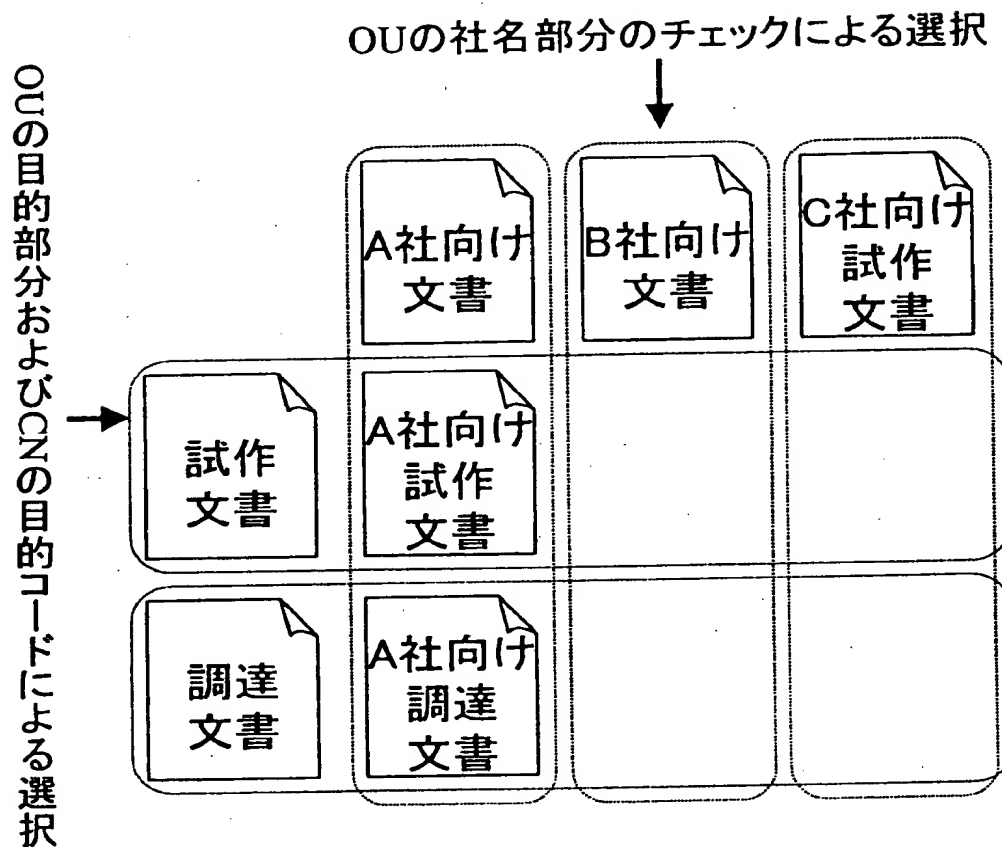
【図 4】



【図 5】



【図 6】



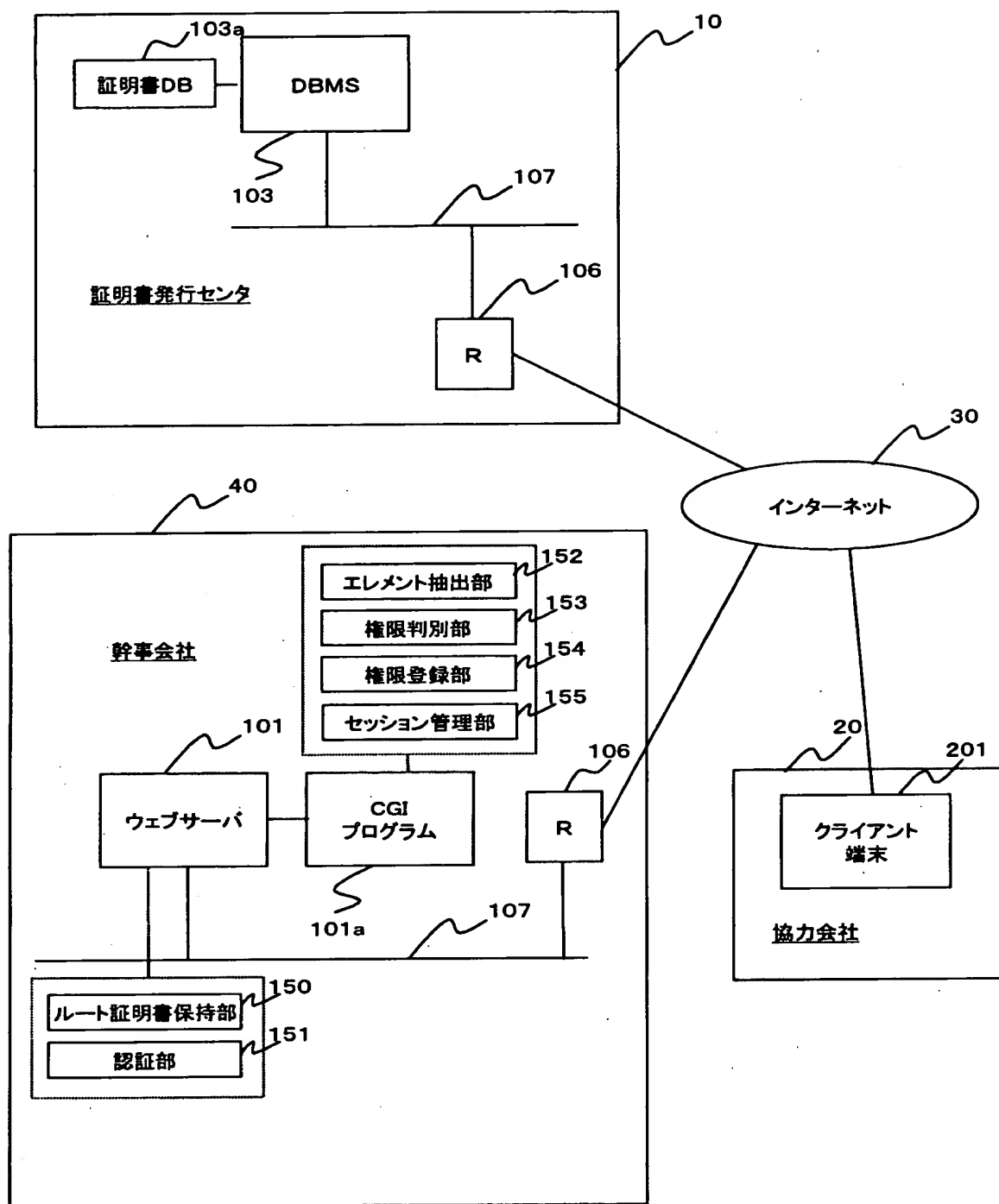
【図 7】

プロジェクト	目的コード	ファイル名／ディレクトリ名

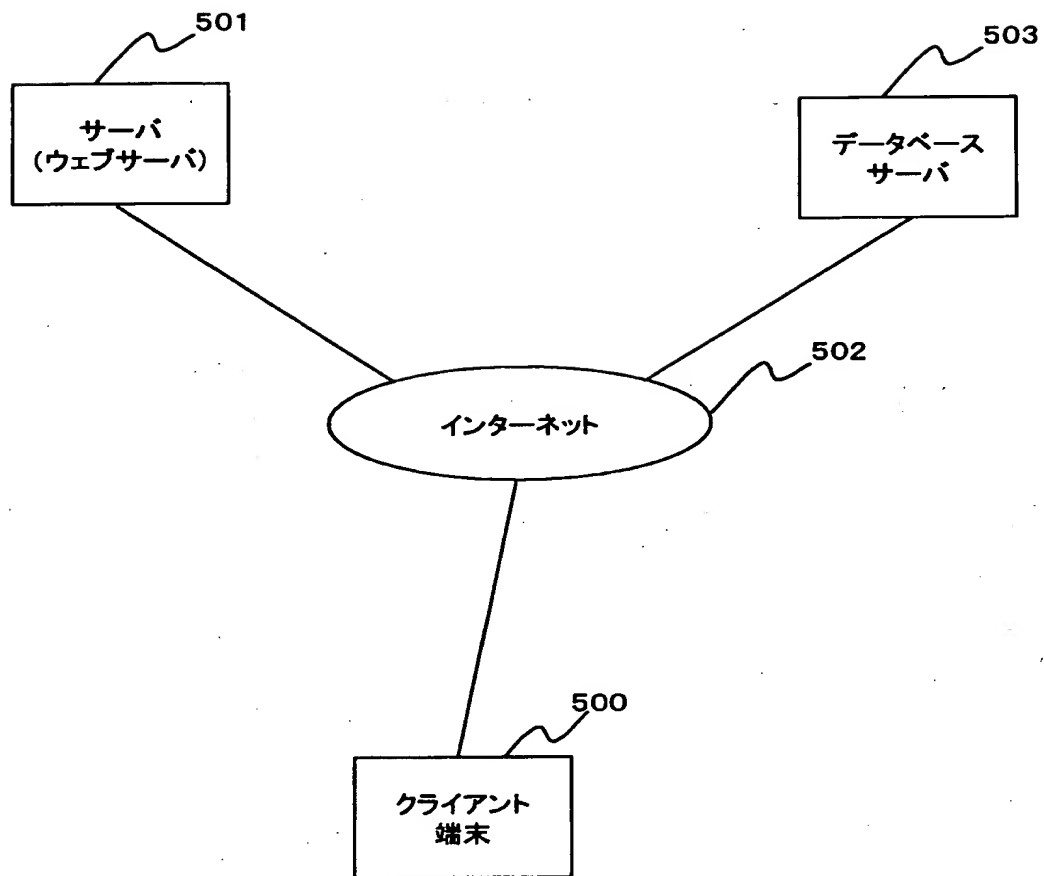
【図 8】

セッション番号	権限（アクセス可能ファイル名／ディレクトリ名）

【図 9】



【図 1 0】



【書類名】 要約書

【要約】

【課題】 証明書のサブジェクト名を利用して簡易にアクセス制御等を行う。

【解決手段】 認証部 1 5 1 は認証手続をクライアント端末 2 0 1 およびウェブサーバ 1 0 1 間で実現する。認証部 1 5 1 は、この認証手続の際に、クライアント端末から証明書を受け取り、そのサブジェクト名がエレメント抽出部 1 5 2 に供給される。エレメント抽出部 1 5 2 はサブジェクト名の階層構造を辿って所定のエレメントを抽出する。権限判別部 1 5 3 は抽出したエレメントの種類、値に基づいて文書のアクセス権限を決定し、これをセッション番号に割り当てる。権限登録部 1 5 4 はセッション番号と権限との関係を登録し以降、セッションが継続する間、このセッション番号に基づいてアクセス権限が許容される。

【選択図】 図 4

出 願 人 履 歴 情 報

識別番号 [000005496]

1. 変更年月日	1996年 5月29日
[変更理由]	住所変更
住 所	東京都港区赤坂二丁目17番22号
氏 名	富士ゼロックス株式会社